Volume 6, Issue 5
May 2024

TLP:CLEAR

FB-ISAO Current Threat Level

FB-ISAO Physical Threat Level:
Elevated

FB-ISAO has assessed the general Physical Threat Level for US Faith-Based Organizations as "ELEVATED." As per FB-ISAO's definitions of the Physical Threat Levels, "ELEVATED" means FB-ISAO is unaware of any specific events, but there is a concern that an event is more likely than normal.

FB-ISAO Cyber Threat Level:
Elevated

FB-ISAO has assessed the general Cyber Threat Level for US Faith-Based Organizations as "ELEVATED." As per FB-ISAO's definitions of the Cyber Threat Levels, "ELEVATED" means FB-ISAO is unaware of any specific events, but there is a concern that an event is more likely than normal.

Stories

How Did the Word Phishing Originate? Page 1

Security Awareness Products: #Didyouknow, Page 2

Spotlight: Beyond FireArms in the House, Page 2

Upcoming Events, Page 2

FB-ISAO Newsletter

How Did the Word Phishing Originate?

According to a Computerworld post by Russell Kay from 2004 (yah! phishing has been around for awhile), "The word *phishing* was coined around 1996 by hackers stealing America Online accounts and passwords. By analogy with the sport of angling, these Internet scammers were using e-mail lures, setting out hooks to "fish" for passwords and financial data from the "sea" of Internet users. Hackers knew that although most users wouldn't take the bait, a few likely would." "Hackers commonly replace the letter *f* with *ph*, a nod to the original form of hacking known as phone phreaking." Phreaking was a telephone system hack from the 1970s. In the late 1990s, hacked accounts were referred to as phish. Hackers traded "phish" for other nefarious tools.

Given all the phish, FB-ISAO regularly shares information to keep you aware of the various phishing themes, tactics, and subjects for you to watch out for. However, it's not practical, or even possible for us to keep you aware of everything, nor for us to expect you to remember it all. Below are some common phishing themes to raise awareness and to help you be on the lookout for "bait".

➤ Finance-themed emails typically have subjects relating to invoices, payments, pay slips, statements, orders, remittances, or receipts.
➤ Notification-themed emails typically have subjects relating to password expiration, reminders, messages, required actions, recent activities, or appointments.
➤ Shipping-themed emails typically have subjects relating to shipments, port information, arrival notices, cargo, or anything to do with DHL, FedEx, UPS, and USPS.
➤ Response-themed emails typically have subjects relating to any sort of response or sometimes forwarded messages as well as hijacked and spoofed email threads. While many threat actors spoof reply chain threads, the most advanced threat actors hijack pre-existing email threads.

Despite all the phish and different ways threat actors use to trick us, there's one thing that's constant – attackers try to elicit a hasty response based on emotion. Fear, urgency, doubt, and curiosity are some of the most common emotions leveraged to pressure us into falling for a phish. Urgent requests for action are often phishing scams.

Here are some simple tips:
➤ Recognize the signs of a phish which may elicit a sense of urgency, contain shortened URLs, and requests to send or verify personal information. *Most notably, AI generated phish emails will not likely contain misspellings, so you'll want to pay closer attention to the other indications.*
➤ Resist the urge to take action on the email. This may be difficult when you are strapped for time.
➤ Report the email to the IT group (if you receive one in a business setting)
➤ Delete the email.

FB-ISAO Advisory Board

Get to Know the Board of Advisors

Contact Us

Email
Info@faithbased-isao.org

Website
www.faithbased-isao.org

Not Yet a Member of FB-ISAO?

How to join…

Not Yet on FB-ISAO Slack? You Need to Be!

Write to membership

Selected Upcoming FB-ISAO Events. Visit the events page for a complete listing.

Office Hours. *(Meeting Invitations sent to all members via email.)*	28 May 2024 at 1pm ET
FireArms in the House: Roundtable and Conclusions	05 June at 12:00pm ET
June 2024 Community Meeting	20 June at 12pm ET

Security Awareness Products: #Didyouknow

In response to a member survey on House of Worship Technology Tools, the Faith Based Information Sharing and Analysis Organization (FB-ISAO) Cyber Threat Intelligence Group is developing a series of products that will be available to the community on our blog site.

The schedule for the product is as follows:

- ➤ June 2024: Streaming Services
- ➤ August 2024: Giving/Offering/Tithing/Donation Sites
- ➤ October 2024: Website Safety
- ➤ December 2024: Social Media Accounts

Each product will describe best practices on the topics and will include tips and parting thoughts and ideas.

The FB-ISAO website also hosts a resource library which is broken up by topic such as securing facilities and people and securing digital assets.

Spotlight: Beyond FireArms in House

The FireArms in the House Program is coming to a close. The last session will be held on 05 June at 12pm ET. The closing session will address any lingering questions not addressed in previous sessions. Member can submit questions to be addressed by the panel.

Your peers and fellow members are already looking ahead to beyond FireArms in the House. The group considered many different ideas and settled on exploring how to build security teams. Planning is already under way – no need to fret – you can still get involved! Whether you have experience relevant to the topic or not, the group needs you!

The planning group meets about twice a month (virtually) and works on planning documents and other planning activities throughout the rest of the month. You can give as little or as much time as you can!

Members who participate often comment about the transfer of knowledge that occurs in the planning sessions – c'mon, give it a try! Write to us and let us know that you'd like to contribute!